

ABSTRACT

Supporting virtual private networks by using a new layer 3 address to encapsulate a network-bound packet so that its context information, from which a layer 2 (e.g., MAC) address can be derived, is preserved. If this encapsulation was not done, the layer 2 address would change over each segment of the network. Thus, the encapsulation preserves the concept of group identification, using at least a part of the context, over the entire network and not just at the edge of the network. If a packet is received from the network (to be forwarded to a customer), the layer 3 address that was added in the encapsulation is stripped off. The original layer 3 destination address may be used with a client device addressing table to determine a new context information, and a layer 2 (e.g., MAC) address of a destination client device. If the client device addressing table does not include entries corresponding to the layer 3 destination address, an address resolution protocol (or "ARP") may be broadcast to request such information or contents of inbound packets may be observed (snooping). The packet may then be forwarded to an aggregation device.